

Ultimo Teorema di Fermat: il mio cent *

Ing. Guido Antonelli

2 gennaio 2006

1 Introduzione

Come tutti gli appassionati di matematica che si rispettino, anch'io ho provato a cimentarmi nella risoluzione della famosa congettura di Pierre de Fermat (1601-1665), impropriamente conosciuta nei secoli passati come Ultimo Teorema di Fermat o *UTF*, approfittando del fatto che, anche se non sono riuscito nell'intento, mi può consolare il fatto di essere in compagnia di molti grandissimi matematici del passato e del presente, che da 300 anni hanno vanamente tentato di trovarne una dimostrazione.

Spero comunque che queste mie note possano servire a tutti coloro che accostandosi per la prima volta a questo argomento, vogliono farsi una semplice idea dell'*UTF*, ed anche di aver apportato qualche piccolo contributo originale all'enorme mole di letteratura esistente sull'argomento.

Nel 1637 Fermat enunciò la sua famosa congettura affermando di possederne una dimostrazione generale, che solo la ristrettezza dei margini del libro del matematico greco Diofanto, sui quali scriveva i propri commenti, non gli permetteva di riportare per esteso.

Tale congettura afferma che l'equazione diofantea¹ di grado n :

$$x^n + y^n = z^n \tag{1}$$

non ammette per x , y e z soluzioni intere non nulle, o più in generale soluzioni razionali non nulle, se l'esponente n è un intero maggiore di 2.

In altre parole si può affermare che la (1) per $n > 2$ ammette nel campo dei numeri interi unicamente soluzioni banali, cioè contenenti uno o più termini nulli.

Di questa congettura, ma solamente per il caso più semplice di $n = 4$, Fermat fornì una elegante dimostrazione provando che in un triangolo rettangolo a lati interi i due cateti non potevano essere quadrati perfetti e che di conseguenza la somma di due quarte potenze, in base al teorema di Pitagora, non avrebbe potuto essere un quadrato, né quindi a maggior ragione una quarta potenza. In seguito Eulero risolse, sia pure in modo non del tutto corretto, il caso $n = 3$, che fu emendato e completato da Sophie Germain, e successivamente altri matematici fino ai giorni nostri dimostrarono la congettura per moltissimi esponenti primi maggiori di 3, senza però arrivare alla dimostrazione generale di cui parlava Fermat.

Benché il problema sia stato recentemente risolto (1995) dal matematico A.Wiles con una dimostrazione che riempie centinaia di pagine di astrusa (almeno per me) algebra moderna, e che quindi l'*UTF* meriti da tale momento a buon diritto la dignità di teorema e non più di semplice congettura, tuttavia resta ancora aperta la questione dell'esistenza o meno di una dimostrazione classica, che avrebbe potuto essere stata alla portata del grande Fermat.

Tra i matematici attualmente sembra comunque prevalere la convinzione che una tale dimostrazione non esista perché altrimenti . . . sarebbe stata certamente trovata!

*Questo articolo è stato scritto con L^AT_EX [1].

¹Si dice diofantea una equazione indeterminata in più incognite, in generale di tipo algebrico, per la quale si ricercano soluzioni unicamente nel campo dei numeri interi.

L'articolo che segue riporta un mio approccio personale al problema, approccio che mi ha permesso di trovare con un procedimento originale tre relazioni a cui qualsiasi eventuale soluzione avrebbe dovuto in ogni caso soddisfare.

Questo risultato mi aveva fatto sperare di poter dimostrare almeno parzialmente l'*UTF*, ma ben presto mi sono accorto che ciò non era vero e che avevo anch'io riscoperto le cosiddette formule di Barlow[2], dal nome del matematico² che per primo le trovò intorno al 1810. Le stesse formule furono poi ottenute indipendentemente da Abel nel 1823 e in seguito da molti altri matematici del secolo scorso.

A queste formule ho aggiunto una quarta relazione che al contrario non risulta citata in [2].

Ho anche trovato e dimostrato un teorema che con poca modestia ho definito *mirabile* per il fatto che interviene in moltissimi punti dei miei ragionamenti.

Vorrei a questo punto aggiungere che nel 1997 avevo scoperto la seguente congettura³, che rappresenta una generalizzazione dell'*UTF*; essa afferma che l'equazione diofantea:

$$x^p + y^q = z^r$$

non ammette soluzioni se x , y e z sono interi non nulli coprimi tra loro, e gli esponenti p , q e r sono interi maggiori di 2. La coprimalità è in questo caso una condizione necessaria altrimenti si avrebbe un immediato controesempio in $2^n + 2^n = 2^{n+1}$ con $n > 2$.

Con un programma elettronico questa congettura è stata da me verificata per tutti i valori dei termini inferiori a 10^{15} , osservando inoltre che se ad uno solo degli esponenti si permettesse di assumere il valore 2, le terne di numeri coprimi che soddisfano a questa equazione resterebbero comunque sempre abbastanza rare (anche se probabilmente infinite!)⁴.

Come diceva Dante *poca favilla gran fiamma seconda*. Mi auguro quindi che qualcuno leggendo questo articolo trovi uno stimolo a proseguire dove io almeno per ora mi sono fermato, ottenendo risultati assai più significativi dei miei.

Infine invito il paziente lettore a segnalarmi eventuali incongruenze od errori da me commessi, cosa peraltro facilissima quando ci si avventura da soli in argomenti di questo tipo.

2 Considerazioni preliminari

Non è necessario dimostrare l'*UTF* per tutti i valori interi dell'esponente n maggiori di 2, ma solamente per $n = 4$ e per quei valori dispari di n che sono anche numeri primi come 3, 5, 7, 11, ecc., numeri cioè che ammettono come divisori esatti solo sé stessi o l'unità.

La dimostrazione è molto semplice e segue dal fatto che ogni numero composto maggiore di 2 o è una potenza esatta di 2, e quindi necessariamente un multiplo di 4, oppure contiene tra i suoi fattori almeno un numero primo dispari:

1. Caso $n = 4k$: possiamo riscrivere la (1) nel modo seguente:

$$(x^k)^4 + (y^k)^4 = (z^k)^4 \quad (k \in \mathcal{N}, \quad k > 0)$$

Se quindi l'*UTF* è vero per $n = 4$ esso risulterà vero anche per $n = 4k$.

2. Caso $n = kp$ ($p =$ numero primo dispari): possiamo riscrivere la (1) nel modo seguente:

$$(x^k)^p + (y^k)^p = (z^k)^p \quad (k \in \mathcal{N}, \quad k > 0)$$

²Personaggio in auge presso il popolo degli astrofili per la famosa lente, di Barlow appunto, da lui inventata.

³Per onestà intellettuale riporto il fatto di essere venuto a conoscenza che questa congettura era già nota prima del 1997, anche se non ne conosco l'autore.

⁴Le terne da me trovate nel campo citato oltre la ben nota relazione $1^n + 2^3 = 3^2$ con $n > 2$, sono le seguenti:

$$\begin{array}{lll} 13^2 + 7^3 = 8^3 & 11^3 + 37^3 = 228^2 & 23^3 + 588^2 = 71^3 & 47^3 + 549^2 = 74^3 \\ 56^3 + 65^3 = 671^2 & 181^2 + 104^3 = 105^3 & 57^3 + 112^3 = 1261^2 & \end{array}$$

Come nel caso precedente, se l'*UTF* è vero per il numero primo p esso risulta vero anche per $n = kp$.

I due casi riportati non si escludono mutuamente nel senso che esistono esponenti come 12, 20, 24, ecc. che sono multipli sia di 4 che di uno o più primi dispari, pur non essendo potenze esatte di 2; per tali valori l'*UTF* è certamente vero, essendo sufficiente il fatto che sia vero per $n = 4$, valore per il quale Fermat, come abbiamo detto, ci lasciò una semplice e convincente dimostrazione.

Il procedimento che in genere si segue per la dimostrazione dell'*UTF* è quello classico per assurdo: si suppone cioè che esista almeno una terna⁵ che soddisfa alla (1) e si cerca di mostrare che tale ipotesi porta ad una conclusione contraddittoria.

Senza perdere di generalità possiamo inoltre imporre le seguenti limitazioni ai valori delle variabili per il caso più interessante di esponente n dispari:

1. I valori x , y e z sono tutti positivi. Infatti, se uno o più valori fossero negativi, potremmo considerarne i relativi opposti positivi eliminando i segni negativi così introdotti mediante spostamento di tali termini da un membro all'altro della formula.
2. I valori x e y sono minori di z . Questo deriva dal fatto che i tre valori, in base al punto precedente, sono supposti positivi e non nulli; possiamo inoltre assumere $x < y$ (se ciò non fosse vero, basta scambiare formalmente tra loro le variabili), escludendo unicamente il caso $x = y$, per il quale si avrebbe $x^p + y^p = 2y^p = z^p$, che non ammette soluzioni intere per y e z in quanto $2^{1/p}$ è irrazionale⁶.
3. I valori x , y e z sono coprimi, cioè primi tra loro. Infatti se x , y e z non fossero coprimi, essi ammetterebbero un massimo comun divisore k , e quindi la (1) sarebbe soddisfatta anche dai valori x/k , y/k e z/k , coprimi tra loro. Una *TdF* coprima è detta fondamentale o primitiva.
4. I valori x , y e z sono primi tra loro anche a coppie. Infatti se x ed y ammettessero un divisore comune k , ponendo $x = ku$ e $y = kv$ con u e v interi positivi, si potrebbe scrivere:

$$k^p (u^p + v^p) = z^p$$

e quindi:

$$(u^p + v^p) = \frac{z^p}{k^p} = \left(\frac{z}{k}\right)^p$$

Ora perché l'ultima espressione sia soddisfatta è necessario che sia anche $z = kw$, con w intero, in contrasto con l'ipotesi iniziale che la terna sia primitiva, che cioè non ammetta un divisore comune diverso da 1. In modo analogo si dimostra facilmente che il ragionamento vale anche per le coppie (x, z) e (y, z) per cui l'asserto risulta così dimostrato.

E' immediato osservare che vale anche la proprietà inversa: se una qualsiasi coppia di variabili di una *TdF* è coprima, allora a maggior ragione anche la terna è coprima; di conseguenza sono coprime anche le altre possibili coppie.

5. Tra i valori x , y e z uno solo può essere pari, mentre i due rimanenti sono necessariamente dispari. Questo fatto si dimostra facilmente con semplici considerazioni sulla parità dei due membri della (1), tenuto conto della coprimalità della terna, oppure più semplicemente dalla precedente osservazione riguardante la coprimalità a coppie.

Non vi sono tuttavia elementi per ritenere che solo x od y possano essere pari, come avviene, e facilmente si dimostra, per le terne pitagoriche (*TdP*) primitive. Pertanto in una eventuale *TdF* anche z potrebbe essere pari.

⁵Le terne in questione sono dette *terne di Fermat* (*TdF*), anche se di fatto non esistono!

⁶Un'altra semplice dimostrazione è la seguente: se $2y^p = z^p$ è verificata da due valori interi y e z coprimi tra loro (se non lo fossero, basterà prima dividerli per il loro MCD), allora z sarà necessariamente pari e di conseguenza z^p conterrà un fattore del tipo 2^{mp} con $m \geq 1$, $p \geq 3$ e quindi $mp \geq 3$. Ma il primo membro contiene solo il fattore 2^1 in quanto y è coprimo con z e quindi dispari. Di conseguenza l'uguaglianza è impossibile c.v.d.

In conclusione, poiché l'*UTF* è stato già dimostrato vero per $n = 4$ resta unicamente da dimostrare che:

$$x^p + y^p = z^p \tag{2}$$

non ammette soluzioni se x, y e z sono interi positivi coprimi con $0 < x < y < z$, e p è un numero primo dispari.

3 Teoremi di Fermat ed Eulero

Pierre de Fermat enunciò anche il seguente (non ultimo) teorema che porta il suo nome: un numero primo p divide esattamente $a^{p-1} - 1$ se a e p sono coprimi. Con formalismo matematico possiamo scrivere:

$$a^{p-1} \bmod p = 1 \quad \text{se : } \text{MCD}(a, p) = 1$$

Successivamente Eulero estese questo teorema anche ai numeri non primi introducendo la funzione toziente $\phi(n)$ di un numero intero n . Tale funzione, intera a sua volta, rappresenta il numero di interi compresi tra 1 e $n - 1$, estremi inclusi, che non hanno alcun divisore⁷ in comune con n .

Il teorema di Eulero rappresenta quindi una generalizzazione di quello di Fermat e viene espresso della seguente relazione:

$$a^{\phi(n)} \bmod n = 1 \quad \text{se : } \text{MCD}(a, n) = 1$$

Nel caso particolare che il numero n sia primo risulta ovviamente $\phi(n) = n - 1$, in quanto un numero primo, non ha fattori comuni con nessuno degli interi compresi tra 1 e $n - 1$, e si ricade così nel teorema di Fermat.

4 Coprimalità e sue proprietà

1. Definizione di coprimalità

Due numeri interi x e y si dicono coprimi se nella loro scomposizione non sono presenti fattori primi comuni, ovvero se $\text{MCD}(x, y) = 1$. Per convenzione il numero 1 si considera sempre coprimo con tutti gli altri numeri.

Questa definizione è resa possibile dal fatto che ogni numero intero è scomponibile in uno ed un solo modo come prodotto di potenze intere di numeri primi⁸ con esponente ≥ 1 .

La coprimalità non gode della proprietà riflessiva (un numero non è mai coprimo con sé stesso), né della proprietà transitiva (se x è coprimo con y ed y è coprimo con z , x non è necessariamente coprimo con z), mentre gode della proprietà simmetrica (se x è coprimo con y , y è coprimo con x).

Come immediata conseguenza della definizione di coprimalità segue il fatto che se due numeri composti sono coprimi, qualsiasi sottomultiplo del primo è coprimo con qualsiasi sottomultiplo del secondo.

⁷In questo caso l'unità non viene considerata tra i possibili divisori di un numero, e viene quindi computata nel calcolo del toziente.

⁸Per garantire l'unicità della scomposizione è necessario che l'unità non venga considerata tra i numeri primi, e si trascuri l'ordine con cui vengono scritti i fattori primi presenti. Con queste precisazioni due numeri interi sono quindi uguali se e solo se si scompongono nello stesso modo.

E viceversa: condizione necessaria e sufficiente perché due numeri composti siano coprimi è che tutti i sottomultipli di ciascun numero siano coprimi con tutti i sottomultipli del secondo numero.

Da queste affermazioni derivano le seguenti proprietà:

2. Proprietà I: Coprimalità del prodotto

Se un numero x è coprimo con y e z allora esso è coprimo anche con il prodotto yz .

3. Proprietà II: Moltiplicazione per costante

Se due numeri x ed y sono coprimi, allora sono ugualmente coprime anche le espressioni hx e ky se $MCD(h, ky) = MCD(k, hx) = 1$.

4. Proprietà III: Variazione di esponenti

Se x ed y sono coprimi, risultano coprime tra loro tutte le coppie di numeri nelle quali il primo ed il secondo numero contengono rispettivamente gli stessi fattori primi di x e di y , anche se con differenti esponenti purché interi positivi o eventualmente nulli.

In particolare, se due numeri x e y sono coprimi, allora sono ugualmente coprimi tutti i numeri interi del tipo x^h e y^k ottenuti elevando x e y a potenza intera o razionale (se il numero così ottenuto è intero).

5. Proprietà IV: Combinazioni lineari

Se due numeri x ed y sono coprimi, allora sono coprime con x ed y , oltre alla somma $x+y$, anche le espressioni:

- $hx + ky$, se $MCD(h, ky) = MCD(k, hx) = 1$
- $hx + y$, se $MCD(h, y) = 1$
- $x + ky$, se $MCD(k, x) = 1$.

6. Proprietà V: Coprimalità di una terna e coprimalità a coppie

Per tre numeri qualsiasi x , y , e z legati dalla relazione $x + y = z$ si hanno le seguenti proprietà di coprimalità:

- Se la terna non è coprima, allora esiste un fattore comune $k = MCD(x, y, z)$ tale che x/k , y/k e z/k rappresentano numeri interi coprimi che soddisfano alla medesima relazione iniziale.
- Se la terna è coprima, allora sono coprime contemporaneamente tutte le coppie ottenibili dalla terna, cioè:

$$MCD(x, y) = MCD(x, z) = MCD(y, z) = 1$$

- Se una qualsiasi coppia di variabili è coprima, allora la terna è coprima e di conseguenza sono coprime per quanto detto al punto precedente anche le altre coppie restanti.

E' interessante osservare che, indipendentemente dalla coprimalità o meno della terna, vale sempre e comunque la relazione:

$$MCD(x, y, z) = MCD(x, y) = MCD(x, z) = MCD(y, z)$$

7. Proprietà VI: Somma/differenza di coprimi di parità diversa

Se due numeri interi x e y sono coprimi e di parità diversa, allora sono coprime tra loro e con x e y anche la loro somma e la loro differenza.

Infatti ponendo:

$$\gamma = y - x \qquad \delta = y + x$$

dalla coprimalità di x ed y in base al punto precedente si deduce che:

$$MCD(\gamma, x) = MCD(\gamma, y) = MCD(\delta, x) = MCD(\delta, y) = 1$$

oltre al fatto che γ e δ sono interi dispari.

Resta ancora da dimostrare che $MCD(\gamma, \delta) = 1$ e per fare questo basta sommare e sottrarre le formule precedenti ottenendo:

$$\delta - \gamma = 2x \qquad \delta + \gamma = 2y$$

Da una qualsiasi di queste relazioni, ad esempio la prima, per la proprietà II si trova che:

$$MCD(\gamma, 2x) = MCD(\gamma, x) = 1$$

poiché $MCD(2, \gamma) = 1$ e di conseguenza la terna è coprima e quindi $MCD(\gamma, \delta) = 1$.

8. Proprietà VII: Semisomma/semidifferenza di coprimi dispari

Se due numeri interi dispari x e y sono coprimi, allora sono coprime tra loro e con x e y anche la loro semisomma e la loro semidifferenza.

Infatti ponendo:

$$\gamma = \frac{y - x}{2} \qquad \delta = \frac{y + x}{2}$$

si ottengono le relazioni:

$$\delta - \gamma = x \qquad \delta + \gamma = y$$

Per dimostrare il teorema è sufficiente dimostrare che $MCD(x, \delta, \gamma) = MCD(y, \delta, \gamma) = 1$ e per fare questo utilizzeremo la proprietà V sulla coprimalità a coppie.

Ad esempio consideriamo γ ed x e dimostriamo che deve essere $MCD(x, \gamma) = 1$.

Supponiamo per assurdo che la tesi sia falsa e che sia $d_x = MCD(x, \gamma) > 1$. Possiamo pertanto scrivere:

$$\frac{\gamma}{d_x} = \frac{y/d_x - x/d_x}{2} = \text{intero}$$

Ora poiché x/d_x è un intero dispari anche y/d_x dovrà essere un intero (dispari), ma questo è assurdo perché y è per ipotesi coprimo con x e quindi non contiene nessuno dei suoi fattori.

In modo analogo possiamo dimostrare che $MCD(y, \gamma) = 1$, e di conseguenza la proprietà in oggetto è dimostrata.

Come casi particolari delle due precedenti proprietà osserviamo che se y è un numero pari, anche $y + 1$ e $y - 1$ sono coprimi tra loro e con y , mentre se y è un numero dispari, anche $(y + 1)/2$ e $(y - 1)/2$ sono coprimi tra loro e con y .

Questi risultati, che si ottengono facilmente con ragionamenti analoghi a quelli sopra riportati, confermano la correttezza di considerare il numero 1 coprimo con tutti gli altri numeri, come già si è fatto per il calcolo del toziente di un numero. Se si accetta questa convenzione, gli stessi risultati derivano immediatamente dai precedenti teoremi ponendo $x = 1$.

5 Questioni di divisibilità

All'equazione (2) possiamo aggiungere la seguente equazione:

$$x + y = z + \alpha \quad (0 < \alpha < x, \quad \alpha \in \mathcal{N}) \quad (3)$$

E' ovvio che questa nuova equazione sembrerebbe a prima vista non portare alcun progresso nel compito che ci siamo proposti in quanto introduce una nuova variabile intera α ; tuttavia nel prosieguo si vedrà che da questa equazione è possibile derivare un certo numero di proprietà a cui le TdF devono soddisfare. L'intervallo di variazione di α è così giustificato:

- $\alpha > 0$ - Tenendo conto della (2), si può scrivere:

$$(x + y)^p = x^p + p x^{p-1} y + \binom{p}{2} x^{p-2} y^2 + \dots + p x y^{p-1} + y^p > x^p + y^p = z^p$$

Estraendo la radice p -esima, segue $x + y > z$ e quindi:

$$\alpha = x + y - z > 0$$

- $\alpha < x$ - Dalla (3) tenendo presente che $y < z$, si ottiene facilmente:

$$\alpha = x + y - z < x + z - z = x$$

1. Fattori del parametro α

Se applichiamo il teorema di Fermat ai vari termini della (2) nell'ipotesi che sia $MCD(x, p) = MCD(y, p) = MCD(z, p) = 1$ avremo per la variabile x :

$$x^p \bmod p = (x^{p-1} \bmod p)(x \bmod p) = x \bmod p$$

e analogamente per le variabili y e z .

Possiamo quindi scrivere la seguente relazione:

$$x \bmod p + y \bmod p = z \bmod p$$

e quindi eliminando l'operazione di modulo ed introducendo il termine additivo α precedentemente visto:

$$x + y = z + \alpha \quad (\alpha = k_p p, \quad k_p \in \mathcal{N}, \quad k_p > 0) \quad (4)$$

La (4) resterebbe valida tuttavia anche se una qualsiasi delle variabili, ad esempio x , fosse divisibile per p , cioè se si avesse ad esempio $MCD(x, p) = p$.

Infatti in questo caso essendo $x^p \bmod p = 0$ procedendo in modo analogo si otterrebbe $y = z + \alpha'$ con $\alpha' = k'_p p = \alpha - x$.

Veniamo ora a considerare tutti i numeri primi q_i che insieme a p soddisfano alla seguente relazione:

$$p - 1 = k (q_i - 1) \quad (k \in \mathcal{N}, \quad k > 0) \quad (5)$$

Applicando l'operazione di modulo rispetto a q_i si avrebbe:

$$x^p \bmod q_i = (x^{q_i-1} \bmod q_i)^k (x \bmod q_i) = x \bmod q_i$$

e analogamente per le variabili y e z .

Ritroviamo quindi relazioni analoghe alla (4), cioè del tipo:

$$x + y = z + \alpha \quad (\alpha = k_{q_i} q_i, \quad k_{q_i} \in \mathcal{N}, \quad k_{q_i} > 0) \quad (6)$$

Come la precedente anche questa relazione resta valida nel caso che una delle variabili x , y o z sia divisibile per q_i .

E' interessante osservare che i valori $q_1 = 2$, $q_2 = 3$ e $q_{max} = p$ saranno sempre presenti in quanto soddisfano la (5) indipendentemente dal valore di p , mentre altri eventuali primi q_i sono invece dipendenti da tale valore.

L'utilizzo del primo $q_1 = 2$ dimostra banalmente il fatto che la parità di un numero o di una espressione non viene modificata se si aggiunge una quantità pari. Infatti la somma $x + y$ uguaglia il valore di z sommato ad una costante pari ($\alpha = 2k_2$).

Più interessante è il fatto che da $q_2 = 3$ si deduce ($\alpha = 3k_3$), cioè la costante α , per qualsiasi valore di $p > 2$ risulta comunque divisibile anche per 3.

Poiché la quantità α è sempre la stessa, possiamo facilmente argomentare che essa deve essere divisibile per tutti i primi q_i che soddisfano alla (5), tra i quali si viene a trovare lo stesso esponente p .

Inoltre avevamo trovato che α doveva essere sempre minore di x , che a sua volta è minore di y . Ponendo $x = y$ troviamo il limite superiore dei valori di x dalla relazione $2x^p = z^p$, per cui si ha $x < z/\sqrt[p]{2}$.

Pertanto, riducendo l'intervallo dei valori possibili di α , possiamo scrivere:

$$\alpha = k \prod q_i \quad \left(\prod q_i \leq \alpha < \frac{z}{\sqrt[p]{2}} - 1, \quad \alpha \in \mathcal{N} \right)$$

dove l'indice i serve a contrassegnare tutti i valori q_i che soddisfano alla (5), valori che sono correlati a p in maniera non semplice..

Purtroppo la presenza di una costante k di proporzionalità ci impedisce di conoscere l'esatta fattorizzazione di α , anche se al punto successivo dimostreremo che il fattore 2 presente in α possiede lo stesso esponente con cui esso è presente nella variabile pari della TdF .

Questo risultato è un caso particolare di una proprietà più generale della scomposizione in fattori di α , argomento questo che verrà ripreso e completato più avanti dopo aver stabilito alcuni importanti lemmi.

2. Scomposizione di somma e differenza di potenze dispari

Riportiamo qui brevemente la nota formula di scomposizione:

$$a^p \pm b^p = (a \pm b) (a^{p-1} \mp a^{p-2}b + a^{p-3}b^2 \mp \dots \mp ab^{p-2} + b^{p-1}) \quad (7)$$

E' interessante osservare che, escludendo il caso che a e b siano entrambi pari, la seconda espressione tra parentesi a secondo membro è sempre e comunque dispari in quanto formata da p termini dispari, se a e b sono entrambi dispari, oppure da $p-1$ termini pari ed un termine dispari nel caso che a e b abbiano differente parità.

Quanto detto vale di conseguenza anche per le coppie formate con le variabili x , y e z , che abbiamo supposto coprime per ipotesi escludendo in tal modo che vi siano 2 variabili pari.

Una seconda osservazione del tutto generale riguarda il fatto che, se a e b sono entrambi dispari, il primo membro $a^p \pm b^p$ sarà necessariamente pari e conterrà quindi un fattore del tipo 2^m . Il medesimo fattore 2^m dovrà necessariamente essere contenuto nell'espressione $(a \pm b)$ in quanto la successiva espressione in parentesi, essendo dispari come detto in precedenza, non può contenere 2 come fattore.

Riferendoci a variabili che fanno parte di una TdF si ottiene un risultato ancora più sorprendente. Supponiamo ad esempio che la variabile pari sia la z e che essa quindi contenga nella sua scomposizione un fattore del tipo 2^m con $m \geq 1$. In questo caso possiamo scrivere:

$$x^p + y^p = z^p = 2^{mp} D_z^p$$

dove $D_z = z/2^m$ è un intero dispari.

Per quanto detto sopra si dovrà avere analogamente:

$$x + y = z + \alpha = 2^{mp} D_{z\alpha}$$

L'ultima uguaglianza può essere così riscritta:

$$2^m D_z + 2^w D_\alpha = 2^{mp} D_{z\alpha}$$

dove si sono introdotte altre costanti dispari, designate mediante la lettera D ed un indice di riferimento, e l'esponente w incognito.

E' facile dimostrare che deve sempre essere $w = m$.

Supponiamo infatti per assurdo che sia $m \neq w$ e mettiamo in evidenza nel primo membro un fattore 2^m :

$$2^m (D_z + D_\alpha 2^{w-m}) = 2^{mp} D_{z\alpha}$$

e quindi:

$$D_z + D_\alpha 2^{w-m} = 2^{m(p-1)} D_{z\alpha}$$

Ora se fosse $w > m$ i due membri avrebbero parità differente e quindi non potrebbero essere uguali, mentre se fosse $w < m$ si avrebbe l'assurdo che il secondo membro intero dovrebbe uguagliare un primo membro contenente il termine frazionario $D_\alpha/2^{m-w}$.

In conclusione resta provato che dovrà essere $m = w$ e quindi si avrà:

$$D_z + D_\alpha = 2^{m(p-1)} D_{z\alpha}$$

concludendo di conseguenza che $D_z + D_\alpha$ è un numero pari contenente il fattore $2^{m(p-1)}$.

Ad analoga conclusione si perviene se la variabile pari è x o y ; si è quindi dimostrato che la costante α non solo è pari ma contiene il fattore 2 con lo stesso esponente m presente nell'unica variabile pari della TdF .

Questo risultato non è valido per le TdP , come si può facilmente verificare, e neppure per le TdF con esponente pari.

3. Un teorema mirabile

A quanto detto al punto precedente può essere data una forma più generale enunciando il seguente mirabile teorema:

In ogni relazione del tipo $x + y = z$ tra numeri interi relativi non nulli, per ciascun fattore primo q , presente con esponente > 0 in almeno uno dei tre termini, esiste sempre almeno un termine che contiene il fattore q^m con il valore massimo m dell'esponente, mentre i restanti due termini contengono un identico fattore q^i con $0 \leq i \leq m$.

In altre parole in una siffatta terna non possono coesistere termini che contengano uno stesso fattore primo con tre diversi esponenti o due soli termini che contengano uno stesso fattore primo con il massimo esponente (ovvero un solo termine che contenga il fattore primo con il minimo esponente).

Per la dimostrazione facciamo l'ipotesi che sia z la variabile che contiene il fattore q^m , mentre per assurdo le variabili x ed y contengono rispettivamente due diversi fattori q^a e q^b con $a < b \leq m$; possiamo allora scrivere:

$$q^a R_x + q^b R_y = q^b \left(\frac{R_x}{q^{b-a}} + R_y \right) = q^m R_z$$

e quindi:

$$\frac{R_x}{q^{b-a}} + R_y = q^{m-b} R_z$$

dove con R_x , R_y ed R_z si sono indicati i resti della fattorizzazione di x , y e z , resti che non contengono più il fattore primo q .

Ma l'ultima uguaglianza è assurda perché il primo membro, a differenza del secondo, non può essere intero per la presenza di R_x/q^{b-a} a meno che non sia $a = b$ c.v.d.

Naturalmente se la generica terna, inizialmente non coprima, viene resa tale dividendo per $MCD(x, y, z)$, si hanno due alternative: o il fattore q scompare da tutte le variabili, se era presente in esse con il medesimo esponente, oppure il fattore q rimane di fatto presente in una sola variabile, mentre nelle altre esso scompare dalla fattorizzazione in quanto avrebbe a questo punto esponente nullo.

Il teorema mirabile generalizzato

Il teorema in oggetto può essere generalizzato sotto due diversi aspetti:

- (a) Generalizzazione rispetto ad x , y e z

I termini considerati dal teorema possono non essere singole variabili, ma anche espressioni comunque complesse, purché sia rispettata la condizione che di ciascun termine si conosca l'esatto esponente con cui il fattore primo q è presente nella scomposizione. Questa estensione è immediata in quanto basta intendere le quantità R_x , R_y ed R_z come resti della scomposizione delle espressioni complesse non contenenti più il fattore primo q .

- (b) Generalizzazione rispetto a q

Il fattore q non deve necessariamente essere un numero primo, ma può essere un qualsiasi numero composto, o al limite un'espressione complessa, alla sola condizione che tutti i fattori primi, presenti nella scomposizione di tale numero od espressione, siano presenti nella relazione solamente in q e nelle sue potenze. Per la dimostrazione basta considerare il fatto che il teorema mirabile è valido separatamente per ciascuno dei singoli numeri primi in cui può essere fattorizzato q ed è quindi valido anche per il loro prodotto.

4. Alcuni rapporti necessariamente interi

Dividendo membro a membro le equazioni (2) e (6) possiamo scrivere:

$$\frac{x^p + y^p}{x + y} = \frac{z^p}{z + \alpha}$$

Poiché la frazione a primo membro è intera, anche la frazione a secondo membro dovrà esserlo, e così le seguenti analoghe frazioni:

$$\frac{z^p - y^p}{z - y} = \frac{x^p}{x - \alpha} \qquad \frac{z^p - x^p}{z - x} = \frac{y^p}{y - \alpha}$$

Inoltre saranno interi anche i seguenti rapporti ottenuti moltiplicando tra loro i precedenti e semplificando mediante la (3):

$$\frac{x^p z^p}{xz - \alpha y} \quad , \quad \frac{y^p z^p}{yz - \alpha x} \quad , \quad \frac{x^p y^p}{xy - \alpha z} \quad \text{e} \quad \frac{x^p y^p z^p}{xyz - \alpha(xz + yz - xy)}$$

6 Lemmi notevoli

1. Lemma I: In una TdF z non può essere né primo né potenza di un primo

Supponiamo per assurdo che sia $z = q^m$ dove q è un numero primo ed m un intero ≥ 1 . In questo caso dovrà essere intero il seguente rapporto:

$$\frac{z^p}{z + \alpha} = \frac{q^{mp}}{q^m + \alpha}$$

La condizione richiesta implica che sia:

$$q^m + \alpha = q^i$$

con $i > m$ in quanto $\alpha > 0$. Si ha quindi per α :

$$\alpha = q^i - q^m = q^m (q^{i-m} - 1) > q^m = z$$

Ma questa conclusione è assurda in quanto $\alpha < x < z$, e pertanto l'ipotesi iniziale è falsa, e il lemma è dimostrato.

2. Lemma II: In una TdF se x è primo o potenza di un primo $\alpha = x - 1$ e $z = y + 1$

Poniamo $x = q^m$ dove q è un numero primo ed m un intero ≥ 1 . In questo caso dovrà essere intero il seguente rapporto:

$$\frac{x^p}{x - \alpha} = \frac{q^{mp}}{q^m - \alpha}$$

La condizione richiesta implica che sia:

$$q^m - \alpha = q^i$$

con $i < m$ in quanto $\alpha > 0$. Si ha quindi per α :

$$\alpha = q^m - q^i = q^i (q^{m-i} - 1)$$

e quindi in questo caso sembrerebbe che α debba contenere anche q tra i suoi fattori.

In realtà non è così perché si può dimostrare che i è nullo e di conseguenza $\alpha = q^m - 1 = x - 1$.

A questo scopo sostituiamo i valori di x ed α nella (3):

$$q^m + y = z + q^m - q^i$$

ottenendo $y = z - q^i$ e quindi $z = q^i + y$.

D'altra parte ricordando la (2) ed il valore di z così trovato, possiamo riscrivere la relazione $x^p = z^p - y^p$ nel modo seguente:

$$\begin{aligned} q^{mp} &= (q^i + y)^p - y^p = \\ &= (q^i)^p + \binom{p}{1} (q^i)^{p-1} y + \dots + \binom{p}{p-2} (q^i)^2 y^{p-2} + \binom{p}{p-1} q^i y^{p-1} + y^p - y^p = \\ &= q^i \left((q^i)^{p-1} + p (q^i)^{p-2} y + \dots + p \frac{p-1}{2} q^i y^{p-2} + p y^{p-1} \right) = \\ &= q^i \left(q^i \left((q^i)^{p-2} + p (q^i)^{p-3} y + \dots + p \frac{p-1}{2} y^{p-2} \right) + p y^{p-1} \right) \end{aligned}$$

In base al teorema mirabile, perché l'uguaglianza sia possibile con riferimento al fattore primo q (q^{mp} è certamente il termine con l'esponente più grande poiché $m > i$), è necessario che i due termini entro le parentesi più esterne contengano la stessa potenza di q e di conseguenza il termine $p y^{p-1}$ dovrebbe contenere il fattore q^i .

Ma escludendo che y^{p-1} possa contenere il fattore q^i in quanto y è coprimo con x e quindi anche con q , perché q^i divida esattamente p si distinguono i due casi seguenti:

- $i \geq 1$ - In questo caso p dovrebbe essere multiplo di q , ma, poiché p è primo, l'unica possibilità porta a concludere che sia $i = 1$ e quindi $p = q$ e $x = p^m$. Ma questa conclusione è impossibile in quanto riprendendo lo sviluppo precedente dopo la sostituzione di q^i con p possiamo mettere in evidenza un termine p^2 ottenendo così:

$$p^{mp} = p^2 \left(p \left(p^{p-3} + p^{p-3} y + \dots + \frac{p-1}{2} y^{p-2} \right) + y^{p-1} \right)$$

Applicando ora nuovamente il teorema mirabile rispetto al fattore primo p si può solamente concludere che la relazione scritta non può essere mai soddisfatta nel campo dei numeri interi e quindi l'ipotesi $i = 1$ è assurda⁹.

⁹E' interessante osservare che tutti i coefficienti binomiali del tipo $\binom{p}{i}$ con p numero primo e $0 < i < p$ sono sempre interi divisibili per p . Infatti, premesso che tali coefficienti sono certamente numeri interi in quanto presenti nello sviluppo della potenza di un binomio, l'espressione:

$$\binom{p}{i} = \frac{p(p-1) \dots (p-i+1)}{i!}$$

contiene necessariamente il fattore p in quanto nessuno dei fattori che costituiscono $i!$, unità a parte, può dividere p per definizione di numero primo. Questa proprietà è caratteristica dei soli numeri primi e potrebbe quindi essere utilizzata per definirli. Inoltre si vede che il fattore p è presente solo con esponente unitario, perché il prodotto dei restanti fattori a numeratore non può essere multiplo di p .

- $i = 0$ - Questa è l'unica possibilità valida restante e corrisponde all'enunciazione del lemma in oggetto, per cui si ha di conseguenza $\alpha = x - 1$ e $z = y + 1$ c.v.d.

Il precedente ragionamento che portava ad escludere che x potesse assumere la forma p^m non sussiste nel caso delle TdP come si può facilmente verificare ponendo $p = 2$ nelle precedenti formule, dalla quali, con semplici passaggi, si ottengono le relazioni:

$$x = 2^m \qquad y = 2^{2(m-1)} - 1 \qquad z = 2^{2(m-1)} + 1$$

che definiscono TdP primitive per ogni valore intero di m maggiore dell'unità.

Si osservi che tali espressioni verificano *identicamente* l'equazione pitagorica che risulta quindi soddisfatta per qualsiasi valore reale o complesso di m . Restando al caso di valori di m interi positivi o nulli si osserva che per $m = 0$ si avrebbero valori frazionari per y e z , mentre per $m = 1$ si ha la soluzione banale $\{2, 0, 2\}$.

Le TdP valide si ottengono quindi solo per $m \geq 2$: per $m = 2$ si ottiene la terna $\{4, 3, 5\}$, per $m = 3$ la terna $\{8, 15, 17\}$, per $m = 4$ la terna $\{16, 63, 65\}$, e così via.

Per quanto riguarda la possibilità che x sia della forma q^m con q primo ma diverso dall'esponente p , le conclusioni per le TdP sono le medesime viste in precedenza per le TdF , esistendo in questo caso una TdP primitiva, per la quale $\alpha = x - 1$ e $z = y + 1$. Questo non esclude l'esistenza di altre TdP non primitive per lo stesso valore della x ; ad esempio per $x = 5^2$ esiste sia la TdP primitiva $\{25, 312, 313\}$, che la TdP non primitiva $\{25, 60, 65\}$.

Si deve inoltre osservare che ad ogni numero primo scelto a piacere corrisponde sempre una (ed una sola) TdP primitiva in cui x assume tale valore; per le TdF invece questo in generale non potrebbe comunque accadere in quanto la relazione $x = \alpha + 1$ permette ad x di assumere solamente valori limitati ai primi di una determinata forma, forma che dipende dai fattori presenti in α ; così ad esempio per $p = 3$ i primi possibili candidati per x sono solo quelli di tipo $6k + 1$, mentre per un generico $p > 3$ dovranno essere comunque scelti tra quelli di tipo $6kp + 1$.

Nel caso delle TdP si ha semplicemente $\alpha = 2k$ e quindi nell'espressione $x = 2k + 1$ sono ricompresi tutti i numeri dispari e di conseguenza tutti i numeri primi.

3. Lemma III: In una TdF y non può essere né primo né potenza di un primo

Supponiamo per assurdo che sia $y = q^m$ dove q è un numero primo. In questo caso dovrà essere intero il seguente rapporto:

$$\frac{y^p}{y - \alpha} = \frac{q^{mp}}{q^m - \alpha}$$

La condizione richiesta implica che sia:

$$q^m - \alpha = q^i$$

con $i < m$ in quanto $\alpha > 0$.

Ripetendo anche in questo caso lo stesso ragionamento fatto per x possiamo affermare che i può unicamente assumere il valore 0 e di conseguenza $\alpha = y - 1$ e $z = x + 1$. Ma queste relazioni sono manifestamente assurde perché in contraddizione con l'ipotesi che sia $x < y < z$ e con la relazione $\alpha < x$ precedentemente dimostrata.

In conclusione l'ipotesi iniziale è falsa ed il lemma è così dimostrato.

4. Lemma IV: x^p , y^p e z^p sono scomponibili nel prodotto di due potenze p -esime coprime

Per dimostrare questo lemma è sufficiente mostrare che è sempre possibile scomporre ciascuna potenza x^p , y^p e z^p nel prodotto simbolico di due termini tra loro coprimi. In conseguenza di questo fatto ogni termine dovrà necessariamente essere una potenza p -esima in quanto i diversi fattori primi in gioco risulteranno presenti in uno solo dei due termini una volta dimostrata la coprialità di questi ultimi.

La dimostrazione porterà anche nel modo più naturale a distinguere il caso in cui nessuna variabile sia divisibile per l'esponente p dal caso in cui vi sia invece una variabile contenente tra i suoi fattori p^m con $m \geq 1$, mostrando che in entrambi i casi tale scomposizione risulta sempre e comunque possibile.

Coerentemente con la definizione di coprialità, se una delle potenze p -esime della scomposizione dovesse valere 1^p , cioè 1, essa sarà considerata coprima con qualsiasi altra potenza p -esima.

Per maggior chiarezza tratteremo separatamente x ed y rispetto a z anche se gli sviluppi dei calcoli sono del tutto simili.

(a) Scomposizione di x^p ed y^p nel prodotto di due potenze p -esime coprime

Per la dimostrazione consideriamo ad esempio la variabile x e per le altre 2 variabili poniamo:

$$z = h + y \quad (8)$$

In base alla proprietà V riguardante la coprialità a coppie si ha $MDC(h, y, z) = 1$ in quanto $MDC(y, z) = 1$ per ipotesi; inoltre, utilizzando questa posizione, la relazione (3) diventa:

$$x = h + \alpha \quad (9)$$

A questo punto sostituendo la (8) nella (2) otteniamo:

$$\begin{aligned} x^p &= (h + y)^p - y^p = \\ &= h^p + \binom{p}{1} h^{p-1} y + \dots + \binom{p}{p-2} h^2 y^{p-2} + \binom{p}{p-1} h y^{p-1} + y^p - y^p = \\ &= h \left(h^{p-1} + p h^{p-2} y + \dots + p \frac{p-1}{2} h y^{p-2} + p y^{p-1} \right) = \\ &= h \left(h \left(h^{p-2} + p h^{p-3} y + \dots + p \frac{p-1}{2} y^{p-2} \right) + p y^{p-1} \right) \end{aligned} \quad (10)$$

Poniamo per comodità:

$$k = h \left(h^{p-2} + p h^{p-3} y + \dots + p \frac{p-1}{2} y^{p-2} \right) + p y^{p-1} \quad (11)$$

scrivendo quindi la precedente relazione come:

$$x^p = h k \quad (12)$$

e domandiamoci ora se h e k , siano o meno coprimi.

Facciamo l'ipotesi che h e k non siano coprimi: esisterà allora certamente un fattore comune $d_{hk} = MCD(h, k) > 1$ per il quale dividere ambo i membri della (11):

$$\frac{k}{d_{hk}} = \frac{h}{d_{hk}} \left(h^{p-2} + p h^{p-3} y + \dots + p \frac{p-1}{2} y^{p-2} \right) + \frac{p y^{p-1}}{d_{hk}}$$

Poiché il primo membro ed il primo termine del secondo membro sono interi, dovrà essere intero anche py^{p-1}/d_{hk} . Ma y^{p-1} non può essere divisibile per d_{hk} in quanto d_{hk} è un fattore di h e $MCD(h, y) = 1$ mentre p , essendo primo, è divisibile solo per sé stesso o per l'unità, per cui si può concludere che h e k o sono coprimi, oppure hanno p come unico fattore comune, cioè $MCD(h, k) = p$.

Nel secondo caso in base alla (12) possiamo facilmente concludere che x deve contenere necessariamente un fattore di tipo p^m con $m \geq 1$, e quindi x^p un fattore p^{mp} ; a loro volta, per la stessa (12), h e k dovranno contenere i fattori p^{mp-1} e p .

Indicando con H e K due quantità tra loro coprime non divisibili per p , potremo distinguere le seguenti due alternative:

- $\begin{cases} h = H p^{mp-1} \\ k = K p \end{cases}$
- $\begin{cases} h = H p \\ k = K p^{mp-1} \end{cases}$

E' facile mostrare che solamente la prima delle due alternative è possibile, in quanto la seconda non può essere vera.

Infatti sostituendo quest'ultima nella (11) si avrebbe:

$$\begin{aligned} K p^{mp-1} &= H p \left((H p)^{p-2} + H^{p-3} p^{p-2} y + \dots + p \frac{p-1}{2} y^{p-2} \right) + p y^{p-1} = \\ &= H p^2 \left(H^{p-2} p^{p-3} + (H p)^{p-3} y + \dots + \frac{p-1}{2} y^{p-2} \right) + p y^{p-1} \end{aligned}$$

Poiché per $p \geq 3$ solamente il termine py^{p-1} contiene il fattore primo p con il minimo esponente, la relazione precedente è certamente falsa in quanto in contraddizione con il teorema mirabile¹⁰.

Al contrario la prima alternativa rispetta i vincoli imposti da tale teorema, come si vede effettuando la sostituzione nella (11):

$$K p = H p^{mp-1} \left((H p^{mp-1})^{p-2} + p (H p^{mp-1})^{p-3} y + \dots + p \frac{p-1}{2} y^{p-2} \right) + p y^{p-1}$$

La stessa procedura può essere seguita per trattare analogamente la variabile y raggiungendo le medesime conclusioni.

Tuttavia x , a differenza di y , presenta la possibilità di essere un primo o la potenza di un primo. In questo caso si avrebbe $h = 1^p = 1$ e le due potenze p -esime, rappresentate da h e h risulterebbero sempre coprime e di conseguenza x non potrebbe essere divisibile per p e questo esclude la possibilità che sia $x = p^m$.

Una verifica immediata di questa conclusione si ottiene ponendo $h = 1$ nella (10):

$$p^{mp} = 1 + p y + \dots + p \frac{p-1}{2} y^{p-2} + p y^{p-1}$$

Si vede infatti che questa relazione è assurda perché il secondo membro, a differenza del primo, non è divisibile per p in quanto la divisione darebbe resto 1.

In conclusione se h e k sono coprimi allora la (12) rappresenta la scomposizione cercata, mentre se h e k ammettono il fattore comune p , allora potremo sempre scrivere:

$$x^p = (p h) \left(\frac{k}{p} \right) \tag{13}$$

¹⁰E' interessante osservare che per $p = 2$ non si raggiunge la stessa conclusione, perché in questo caso si avrebbe:

$$K 2^{2m-1} = 2H + 2y$$

che è una relazione perfettamente in linea con il teorema mirabile.

evidenziando così con le parentesi i due termini coprimi.

Abbiamo quindi dimostrato che indipendentemente dal fatto che p divida o meno x è sempre possibile scomporre la potenza x^p nel prodotto di due termini tra loro coprimi e questa coprimalità ha come immediata conseguenza il fatto che tali termini devono a loro volta essere potenze p -esime come si era detto all'inizio del paragrafo.

Analoga conclusione vale anche per la y tenendo comunque conto che solo una delle 3 variabili di una TdF primitiva può essere divisibile per p .

(b) Scomposizione di z^p nel prodotto di due potenze p -esime coprime

La dimostrazione è molto simile alla precedente. La posizione iniziale sarà ora:

$$x = h - y \quad (14)$$

Anche in questo caso si ha $MDC(h, x, y) = 1$ in quanto $MDC(x, y) = 1$ per ipotesi; inoltre, utilizzando questa posizione, la relazione (3) diventa:

$$z = h - \alpha \quad (15)$$

A questo punto sostituendo la (14) nella (2) otteniamo:

$$\begin{aligned} z^p &= (h - y)^p + y^p = \\ &= h^p - \binom{p}{1} h^{p-1} y + \dots - \binom{p}{p-2} h^2 y^{p-2} + \binom{p}{p-1} h y^{p-1} - y^p + y^p = \\ &= h \left(h^{p-1} - p h^{p-2} y + \dots - p \frac{p-1}{2} h y^{p-2} + p y^{p-1} \right) = \\ &= h \left(h \left(h^{p-2} - p h^{p-3} y + \dots - p \frac{p-1}{2} y^{p-2} \right) + p y^{p-1} \right) \end{aligned}$$

Da questo punto in avanti la dimostrazione prosegue come si è visto in precedenza per x tenendo presente che z , in base al lemma I, non può mai essere primo o potenza di primo. Si osservi che l'espressione racchiusa tra le parentesi più interne non può mai annullarsi in quanto porterebbe ad avere $z^p = h p y^{p-1}$ che è in contraddizione con il fatto che z ed y sono coprimi.

In conclusione ciascuno dei termini della (2) può essere scritto come prodotto di due potenze p -esime coprime:

$$x^p = u_x^p v_x^p \quad y^p = u_y^p v_y^p \quad z^p = u_z^p v_z^p \quad (16)$$

dove le variabili introdotte, se x , y e z non sono divisibili per p , hanno i seguenti valori:

$$\begin{aligned} u_x^p &= z - y & v_x^p &= (z^{p-1} + z^{p-2} y + \dots + z^2 y^{p-3} + z y^{p-2} + y^{p-1}) \\ u_y^p &= z - x & v_y^p &= (z^{p-1} + z^{p-2} x + \dots + z^2 x^{p-3} + z x^{p-2} + x^{p-1}) \\ u_z^p &= x + y & v_z^p &= (x^{p-1} - x^{p-2} y + \dots + x^2 y^{p-3} - x y^{p-2} + y^{p-1}) \end{aligned} \quad (17)$$

Nel caso invece che una delle variabili sia divisibile per p , delle sei precedenti relazioni risultano modificate solo le due relative a tale variabile (la x nell'esempio che segue), mentre le altre quattro restano inalterate:

$$\begin{aligned} u_x^p &= p(z - y) & v_x^p &= (z^{p-1} + z^{p-2} y + \dots + z^2 y^{p-3} + z y^{p-2} + y^{p-1})/p \\ u_y^p &= (z - x) & v_y^p &= (z^{p-1} + z^{p-2} x + \dots + z^2 x^{p-3} + z x^{p-2} + x^{p-1}) \end{aligned} \quad (18)$$

$$u_z^p = (x + y) \quad v_z^p = (x^{p-1} - x^{p-2}y + \dots + x^2y^{p-3} - xy^{p-2} + y^{p-1})$$

Se la variabile divisibile per p fosse stata la y o la z si sarebbe invece dovuto modificare le due relazioni della seconda o della terza riga¹¹.

Resta quindi dimostrato completamente il lemma in oggetto.

E' molto interessante confrontare i risultati con quelli che si ottengono per l'equazione pitagorica cioè nel caso $p = 2$. Una prima osservazione consiste nel fatto che z^2 , essendo somma di due quadrati, non è scomponibile come gli altri termini x^2 ed y^2 . In secondo luogo si deve osservare che tra x ed y vi è sempre e comunque una variabile pari, cioè divisibile per 2, che nel caso presente viene a coincidere proprio con l'esponente p .

Prendendo per comodità a riferimento la variabile x si hanno quindi due casi:

(a) La variabile x è dispari.

$$x^2 = (z - y)(z + y) = m^2 n^2$$

La proprietà VI riportata nelle pagine precedenti ci garantisce che i due termini in parentesi siano coprimi e quindi possiamo scrivere:

$$(z - y) = m^2 \quad (z + y) = n^2$$

da cui si deriva una prima versione delle formule risolutive di Diofanto con m ed n coprimi, entrambi dispari ed $n > m$.

(b) La variabile x è pari.

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z - y}{2}\right)\left(\frac{z + y}{2}\right) = m^2 n^2$$

La proprietà VII riportata nelle pagine precedenti ci garantisce che i due termini in parentesi siano coprimi e quindi possiamo scrivere:

$$\left(\frac{z - y}{2}\right) = m^2 \quad \left(\frac{z + y}{2}\right) = n^2$$

da cui si deriva una seconda versione delle formule risolutive di Diofanto con m ed n coprimi, di parità diversa ed $n > m$.

Non è invece lecito utilizzare i risultati trovati in precedenza per le TdF nel caso che la variabile considerata sia divisibile per l'esponente e scrivere:

$$x^2 = \left(2(z - y)\right)\left(\frac{z + y}{2}\right) = m^2 n^2$$

da cui si potrebbe ricavare:

$$2(z - y) = m^2 \quad \left(\frac{z + y}{2}\right) = n^2$$

Anche se è possibile ottenere delle soluzioni all'equazione pitagorica, il ragionamento seguito è errato perché le considerazioni sulla parità fatte in base alla formula di scomposizione (7) valgono solo per esponenti dispari.

¹¹Nella prima delle (18) si è scelta la soluzione più semplice portando p in u_x . L'alternativa sarebbe stata:

$$u_x^p = (z - y)/p^{mp-1} \quad v_x^p = p^{mp-1}(z^{p-1} + z^{p-2}y + \dots + z^2y^{p-3} + zy^{p-2} + y^{p-1})$$

e analogamente se le variabili divisibili per p fossero state la y o la z .

7 Fattorizzazione del parametro α

Sulla base di quanto visto al paragrafo precedente si è stabilita la possibilità di spezzare la scomposizione in fattori di ciascuna delle tre variabili x , y e z in due parti separate coprime tra loro. Infatti dalle (16), estraendo la radice p -esima, si ottiene immediatamente:

$$x = u_x v_x \quad y = u_y v_y \quad z = u_z v_z \quad (19)$$

Dobbiamo a questo punto distinguere i due possibili casi:

1. Nessuna variabile della TdF è divisibile per p

Utilizzando le (17), la (3) e le (19) possiamo scrivere le seguenti relazioni:

$$u_x^p = z - y = x - \alpha = u_x v_x - \alpha$$

$$u_y^p = z - x = y - \alpha = u_y v_y - \alpha$$

$$u_z^p = x + y = z + \alpha = u_z v_z + \alpha$$

Ora l'applicazione del teorema mirabile generalizzato richiede necessariamente che il parametro α , in base alla prima delle tre relazioni, contenga u_x tra i suoi fattori, in base alla seconda u_y e in base alla terza u_z , e che quindi possa scriversi:

$$\alpha = A_p p^m u_x u_y u_z = A_p p^m \sqrt[p]{(z-y)(z-x)(x+y)} \quad (20)$$

Si osservi nella precedente formula l'aggiunta di un fattore p^m , con $m \geq 1$, sulla base del fatto che α deve essere sempre e comunque divisibile per p , come è stato dimostrato mediante il teorema di Fermat.

Riguardo al fattore di proporzionalità A_p introdotto, si può con certezza affermare che esso non può contenere nessuno dei fattori primi presenti in u_x , u_y e u_z , sempre per il già citato teorema mirabile¹².

2. Una delle variabili della TdF è divisibile per p

Supponendo che sia x la variabile divisibile per p , utilizzando la prima delle (18) avremo:

$$u_x^p = p(z-y) = p(x-\alpha) = p u_x v_x - p \alpha \quad (21)$$

mentre le altre due relazioni restano invariate:

$$u_y^p = z - x = y - \alpha = u_y v_y - \alpha$$

$$u_z^p = x + y = z + \alpha = u_z v_z + \alpha$$

Mentre queste ultime implicano che α sia multiplo di u_y e u_z , per la (21) si deve partire dal considerare tutti i fattori di u_x ad eccezione di p . Questi fattori saranno certamente presenti in α con gli stessi esponenti con cui sono presenti in u_x .

Mettiamo ora in evidenza nella (21) le potenze di p :

$$p^{mp} \left(\frac{u_x^p}{p^{mp}} \right) = p p^m \left(\frac{u_x}{p^m} \right) v_x - p \alpha$$

¹²Come si vedrà più avanti A_p è una funzione di p , x , y e z che non potrà comunque avere 2 tra i suoi fattori in quanto uno dei termini sotto radice è certamente pari.

I termini tra parentesi sono interi e coprimi con p e quindi il teorema mirabile ci dice che α deve contenere lo stesso fattore p^m contenuto in u_x . Pertanto la conclusione finale risulta identica al caso precedente, cioè u_x è un fattore di α .

Possiamo perciò scrivere:

$$\alpha = A_p u_x u_y u_z = A_p \sqrt[p]{p(z-y)(z-x)(x+y)} \quad (22)$$

Si può osservare che in questo caso non è più necessario, e sarebbe un errore, aggiungere il fattore p esternamente alla radice in quanto $\sqrt[p]{p(z-y)}$ fornisce già ad α tale fattore. E' inoltre significativo il fatto che l'espressione finale di α resta invariata qualora la variabile divisibile per p sia y o z invece che x .

In conclusione il termine α contiene sempre e comunque una parte dei fattori di ciascuna delle variabili x , y e z e proprio con gli stessi esponenti presenti nelle variabili stesse; questa caratteristica di α è condizione necessaria perché $x^p/(x-\alpha)$, $y^p/(y-\alpha)$ e $z^p/(z+\alpha)$ possano essere quantità intere¹³.

Resta ora da discutere quale delle due relazioni, tra la (20) e la (22), sia corretta o se lo siano entrambe, e da analizzare quale possa essere il valore del fattore A_p e se e come tale valore venga a dipendere da p .

8 Espressione analitica del parametro α

Nel paragrafo precedente abbiamo osservato come il parametro α possa rappresentarsi mediante due differenti espressioni, la (20) e la (22) a seconda che una delle variabili della TdF sia divisibile o meno per l'esponente p . Quest'ultima distinzione è stata considerata talmente importante nella storia dei tentativi di soluzione dell' UTF che tradizionalmente si parla rispettivamente di *primo caso* e *secondo caso* dell' UTF a seconda che p non divida o divida il prodotto xyz , dove x , y e z rappresentano una TdF coprime¹⁴.

Per decidere quale sia la formula corretta e come si possa esprimere in forma simbolica il fattore intero A_p si deve ricorrere alla seguente identità algebrica scoperta da Lamé nel 1840, qui riportata nella forma datagli successivamente da Werebrusow[2] e da me modificata secondo i simboli e le convenzioni adottate:

$$(x+y-z)^p - (x^p + y^p - z^p) = \left[\frac{(p-1)!}{2^{p-2}} \cdot \sum \frac{(z-y)^{2i} (z-x)^{2j} (x+y)^{2k}}{(2i+1)! (2j+1)! (2k+1)!} \right] p (z-y)(z-x)(x+y) \quad (23)$$

dove la sommatoria deve considerarsi estesa a tutti i valori interi $i, j, k \geq 0$ che soddisfano alla condizione $i + j + k = (p-3)/2$.

Ora è possibile passare immediatamente da questa identità ad una equazione perfettamente equivalente alla forma canonica dell' UTF . Infatti per una qualsiasi TdF il termine a primo membro $(x^p + y^p - z^p)$ è ovviamente nullo, e quindi, estraendo la radice p -esima di ciascun membro, otteniamo la relazione:

$$x + y - z = \alpha = \sqrt[p]{\frac{(p-1)!}{2^{p-2}} \cdot \sum \frac{(z-y)^{2i} (z-x)^{2j} (x+y)^{2k}}{(2i+1)! (2j+1)! (2k+1)!}} \sqrt[p]{p} \sqrt[p]{(z-y)(z-x)(x+y)} \quad (24)$$

¹³Solo per la variabile x il fattore comune u_x assume valore 1 quando x è primo o potenza di primo.

¹⁴Se la terna è coprime, solo una delle variabili è divisibile per p nel secondo caso dell' UTF .

Possiamo pertanto affermare che x , y e z costituiscono una TdF se sono numeri interi positivi che soddisfano alla (24).

Dalla stessa (24) si ricava l'espressione simbolica di A_p :

$$A_p = \sqrt[p]{\frac{(p-1)!}{2^{p-2}} \cdot \sum \frac{(z-y)^{2i} (z-x)^{2j} (x+y)^{2k}}{(2i+1)! (2j+1)! (2k+1)!}} \quad (25)$$

Dal confronto della (24) con la (20) e la (22) sembra quindi doversi concludere che il parametro α è espresso correttamente solo dalla (22) e questo porterebbe a concludere che il primo caso dell' UTF sarebbe sempre vero per qualsiasi valore di p .

Purtroppo questa conclusione non è corretta, anche se nei ragionamenti successivi essa risulta valida per il solo caso $p = 3$.

Si osservi che appositamente nella (24), a differenza della (22), si è isolato il fattore $\sqrt[p]{p}$, per ragioni che vedremo di seguito, malgrado che esso sia irrazionale e quindi non intero.

Proviamo ora ad esplicitare la (24) per i primi tre valori dell'esponente p , cioè $p = 3, 5, 7$, ed infine analizziamo il caso pitagorico $p = 2$.

1. Valore di A_p ed α nell'equazione di Fermat per $p = 3$

Invece di utilizzare la (25) per $p = 3$ con cui si troverebbe direttamente il valore $A_3 = 1$, mostriamo che lo stesso risultato si potrebbe ottenere più semplicemente utilizzando la (3) e la (22) nel modo seguente:

$$x + y - z = A_3 \sqrt[3]{3(z-y)(z-x)(x+y)}$$

Lo sviluppo di $(x + y - z)^3$ fornisce la seguente espressione:

$$x^3 + y^3 - z^3 + 3xy^2 + 3x^2y + 3xz^2 + 3yz^2 - 3x^2z - 3yz^2 - 6xyz$$

mentre quello di $A_3^3 (3(z-y)(z-x)(x+y))$ è invece:

$$A_3^3 (3xy^2 + 3x^2y + 3xz^2 + 3yz^2 - 3x^2z - 3yz^2 - 6xyz)$$

Dal confronto appare quindi evidente che poiché la somma $x^3 + y^3 - z^3$ è nulla per ipotesi, dovrà aversi $A_3^3 = 1$, cioè $A_3 = 1$, e quindi il valore di α sarà:

$$\alpha = \sqrt[3]{3(z-y)(z-x)(x+y)}$$

Quest'ultima relazione dimostra che per $p = 3$ il primo caso dell' UTF è certamente vero. Infatti $\sqrt[3]{3}$ non è intero mentre α lo deve essere; di conseguenza $\sqrt[3]{3}$ dovrà comunque legarsi ad uno qualsiasi dei termini sotto radice cubica e di conseguenza, per quanto visto al paragrafo 6, almeno una delle variabili della TdF deve essere divisibile per 3.

2. Valore di A_p ed α nell'equazione di Fermat per $p = 5$ e $p = 7$

Se si procedesse come per il caso precedente, il problema per $p = 5$ si complicherebbe a causa dello sviluppo di $(x + y - z)^5$ che contiene già 21 termini¹⁵.

E' quindi più conveniente utilizzare la (25) che permette di trovare per la costante A_5 la seguente espressione:

$$A_5 = \sqrt[5]{\frac{1}{2} \left((z-y)^2 + (z-x)^2 + (x+y)^2 \right)} \quad (26)$$

¹⁵Il numero dei termini nel caso generale è uguale a $(p+1)(p+2)/2$.

Dopo calcoli ancora più laboriosi, si è trovata l'espressione di A per $p = 7$:

$$A_7 = \sqrt[7]{\frac{1}{2} \left((z-y)^4 + (z-x)^4 + (x+y)^4 + 10xyz(x+y-z) \right)}$$

L'espressione di α si ottiene poi naturalmente moltiplicando il fattore A_p così trovato per l'espressione $\sqrt[p]{(z-y)(z-x)(x+y)}$ con $p = 5$ o $p = 7$ rispettivamente.

A questo punto dobbiamo chiederci perché la conclusione trovata per $p = 3$, cioè la dimostrazione del primo caso dell'*UTF*, non possa essere estesa agli altri valori di p .

La ragione di ciò consiste nel fatto che A_p per $p > 3$ è sempre diverso da 1 e quindi il fattore $\sqrt[p]{p}$, irrazionale e comunque non intero, potrebbe legarsi ad A_p invece che ad una delle 3 espressioni $(z-y)$, $(z-x)$ o $(x+y)$ per poter dare origine ad un valore intero. Questa ipotesi, corrispondente al primo caso dell'*UTF*, comporta che A_p contenga necessariamente nella sua scomposizione il fattore $p^{m^{p-1}}$ con $m \geq 1$.

3. Valore di A_p ed α nell'equazione di Pitagora per $p = 2$

I ragionamenti fatti in precedenza non sono validi per esponenti pari in quanto $x^n + y^n$ non è divisibile per $x + y$ e quindi il termine $x + y$ non potrebbe comparire sotto radice.

Consideriamo quindi il caso pitagorico, ignorando tale termine e tenendo presente che vi sarà sempre una variabile tra x ed y divisibile per l'esponente 2.

Riscriviamo quindi la (3) nel modo seguente:

$$x + y = z + A_2 \sqrt{2(z-y)(z-x)}$$

Spostando z a primo membro ed elevando al quadrato, si ottiene:

$$x^2 + y^2 + z^2 + 2xy - 2xz - 2yz = A_2^2(2z^2 + 2xy - 2xz - 2yz)$$

E' immediato verificare che per $A_2 = 1$ si ottiene, come era lecito attendersi, proprio l'equazione pitagorica $x^2 + y^2 = z^2$, soddisfatta per ipotesi, e di conseguenza:

$$\alpha = u_x u_y = \sqrt{2(z-y)(z-x)}$$

Sostituendo le formule classiche di risoluzione $x = 2nm$, $y = m^2 - n^2$ e $z = m^2 + n^2$ con m ed n coprimi di diversa parità ed $m > n$, si ottiene:

$$\alpha = u_x u_y = \sqrt{4n^2(m-n)^2} = 2n(m-n)$$

Quest'ultimo risultato mostra che se m e n sono interi anche l'espressione simbolica di α corrisponde ad un'espressione polinomiale intera nelle stesse variabili, come ci si poteva logicamente attendere.

Purtroppo per $n > 2$ non esistono formule analoghe prive di termini radicali, né per α né per le variabili incognite x , y e z .

9 Riscoperta delle formule di Barlow

A questo punto, come molti altri matematici per professione e per passione (Abel, Legendre, Germain, Lindemann, Catalan, ed altri), anch'io sono giunto ora, sulla base di quanto precedentemente esposto, a riscoprire e dimostrare quelle relazioni, note con il nome di formule di Barlow (1810, 1811), a cui tutte le *TdF* devono soddisfare.

A queste relazioni ho poi aggiunto per $p > 3$ una ulteriore condizione di vincolo, come si vedrà da quanto segue.

Infatti, prescindendo per ora dal fattore p , quando si è dedotta la fattorizzazione del parametro α , è stato osservato che, per il teorema mirabile generalizzato, u_x , u_y , u_z e A_p dovevano essere tutte quantità prime tra loro.

Di conseguenza, se ciascuno di questi termini viene rappresentato, come appare nella (24), mediante la radice p -esima di un'espressione funzione di x , y e z , tale espressione deve essere necessariamente una potenza p -esima esatta in modo da dare origine, dopo l'estrazione di radice, ad un valore intero. Per quanto riguarda il fattore $\sqrt[p]{p}$ presente nella (24), esso dovrà associarsi ad una delle quattro quantità sopra viste, la quale, numericamente parlando, dovrà contenere sotto radice p -esima un fattore di tipo p^{mp-1} . In altri termini questa quantità, a differenza delle altre, diventerà una potenza p -esima esatta solo inglobando sotto radice un fattore p .

1. Primo caso dell'UTF (p non divide xyz)

In questo caso $\sqrt[p]{p}$ deve essere associata al fattore A_p e quindi, introducendo quattro parametri coprimi r , s , t ed w , possiamo scrivere:

$$\begin{aligned} z - y &= r^p \\ z - x &= s^p \\ x + y &= t^p \end{aligned} \tag{27}$$

$$\frac{p!}{2^{p-2}} \cdot \sum \frac{(z-y)^{2i} (z-x)^{2j} (x+y)^{2k}}{(2i+1)! (2j+1)! (2k+1)!} = w^p$$

Nel primo membro dell'ultima relazione si è inglobato il fattore p in $p!$.

Dalle prime tre relazioni delle (28) si ricavano le formule di Barlow:

$$\begin{aligned} x &= \frac{1}{2}(t^p - s^p + r^p) \\ y &= \frac{1}{2}(t^p + s^p - r^p) \\ z &= \frac{1}{2}(t^p + s^p + r^p) \end{aligned} \tag{28}$$

L'interpretazione di queste formule è la seguente: se il primo caso dell'UTF possiede soluzioni, queste devono essere esprimibili mediante le (29) in funzione di tre parametri coprimi r , s , e t , di cui uno pari, non divisibili per p .

La quarta delle (28) impone un ulteriore vincolo tra questi tre parametri ed il quarto parametro w , che oltre ad essere dispari, a differenza dei precedenti, dovrà essere divisibile per p .

$$\frac{p!}{2^{p-2}} \cdot \sum \frac{r^{2pi} s^{2pj} t^{2pk}}{(2i+1)! (2j+1)! (2k+1)!} = w^p$$

2. Secondo caso dell'UTF (p divide xyz)

In questo caso $\sqrt[p]{p}$ non sarà più associato ad A_p ma ad uno dei tre termini in parentesi della (22) che compaiono sotto la radice p -esima, e precisamente a quello corrispondente alla variabile divisibile per p . Supponendo che sia x tale variabile e che di conseguenza p sia associato al termine $(z - y)$, possiamo scrivere:

$$\begin{aligned} p(z - y) &= r^p \\ z - x &= s^p \\ x + y &= t^p \end{aligned} \tag{29}$$

$$\frac{(p-1)!}{2^{p-2}} \cdot \sum \frac{(z-y)^{2i} (z-x)^{2j} (x+y)^{2k}}{(2i+1)! (2j+1)! (2k+1)!} = w^p$$

E' interessante osservare come la prima relazione fornisca un'ulteriore conferma al fatto che x non può mai essere una potenza di p . Infatti, avendosi in questo caso $z-y=1$, si avrebbe di conseguenza $p=r^p$, relazione chiaramente assurda.

Risolvendo il sistema lineare in questione, si ottengono le seguenti espressioni:

$$\begin{aligned} x &= \frac{1}{2} \left(t^p - s^p + \frac{1}{p} r^p \right) \\ y &= \frac{1}{2} \left(t^p + s^p - \frac{1}{p} r^p \right) \\ z &= \frac{1}{2} \left(t^p + s^p + \frac{1}{p} r^p \right) \end{aligned} \quad (30)$$

Se p fosse invece associato al termine $z-x$ oppure $x+y$ le precedenti relazioni richiederebbero unicamente lo spostamento del fattore $1/p$ da r^p a s^p o a t^p rispettivamente.

In modo analogo al caso precedente l'interpretazione di queste formule è la seguente: se il secondo caso dell' UTF possiede soluzioni, queste devono essere esprimibili mediante le (31) in funzione di tre parametri coprimi $r, s, e t$, di cui uno pari ed uno divisibile per p (in questo caso x).

La quarta delle (30) impone un ulteriore vincolo tra questi tre parametri ed il quarto parametro w , che oltre ad essere dispari è coprimo con gli altri e non divisibile per p .

$$\frac{(p-1)!}{2^{p-2}} \cdot \sum \frac{r^{2pi} s^{2pj} t^{2pk}}{(2i+1)! (2j+1)! (2k+1)!} = w^p$$

A quanto detto va aggiunta un'ulteriore osservazione: poiché nella (22) A_p ed il successivo termine sotto radice sono coprimi per il teorema mirabile generalizzato, e A_p deve essere intero, allora dalla (26) per $p=5$ si dovrà avere:

$$\frac{1}{2} \left((z-y)^2 + (z-x)^2 + (x+y)^2 \right) = \frac{1}{2} \left(\frac{1}{25} r^{10} + s^{10} + t^{10} \right) = w^5$$

essendo w un intero dispari coprimo con r, s e t .

Questa relazione rappresenta un ulteriore vincolo per le TdF anche se non appare semplice utilizzarla per i nostri scopi. Analoghe relazioni possono scriversi per esponenti p maggiori di 5.

E' interessante osservare che anche α può essere espresso in funzione dei tre nuovi parametri:

$$\alpha = x + y - z = \frac{1}{2} \left(t^p - s^p - \frac{1}{p} r^p \right)$$

Ma α è anche dato dalla (22), dove anche la costante A_p è esprimibile in funzione di p e dei tre parametri. Si ha quindi:

$$\frac{1}{2} \left(t^p - s^p - \frac{1}{p} r^p \right) = A_p(p, r, s, t) \cdot r s t$$

Per $p=3$ la relazione precedente risulta assai semplice:

$$\frac{1}{2} \left(t^3 - s^3 - \frac{1}{3} r^3 \right) = r s t$$

Può essere interessante vedere che cosa accade per $p=2$. Le relazioni corrispondenti alle (30) diventerebbero:

$$\begin{aligned} 2(z-y) &= r^2 & (r, s \text{ coprimi, } x, r \text{ pari}) \\ z-x &= s^2 \end{aligned}$$

Da queste relazioni si ricava la condizione, necessaria ma non sufficiente, $y-x = s^2 - r^2/2$ per x pari (e $y-x = s^2/2 - r^2$ per x dispari), che è sempre e comunque verificata da ogni TdP .

10 Conclusioni

E' indubbiamente molto difficile trarre delle conclusioni da quanto scritto.

Purtroppo l'*UTF* ha resistito e ancora resiste dopo trecento anni a qualsiasi tentativo di risoluzione con i metodi cosiddetti euleriani, mentre la soluzione trovata da Wiles resta con mio rammarico riservata solo a pochi iniziati.

Le note che ho scritto appariranno certamente al molto paziente lettore piuttosto disordinate, anche se ho tentato di riordinarle al meglio prima di esporre in pubblico questo scritto. Ciò è dovuto al fatto che esse hanno seguito il flusso dei miei ragionamenti via via che mi si presentavano alla mente; inoltre molte altre direzioni sono state da me esplorate ma non riportate in quanto prive di un qualsiasi sbocco significativo.

Un'idea guida intuibile in alcuni dei miei ragionamenti che vorrei lasciare a chi mi seguirà in questa ricerca divertente ed appassionante, è basata su domande di questo tipo:

Perché esistono infinite *TdP* e non esiste nessuna *TdF*?

Quali differenze comportano esponenti maggiori di 3 rispetto all'esponente 2 delle terne pitagoriche?

Questo è il motivo per cui talvolta confrontavo tra loro le *TdP* e le *TdF* mettendo in evidenza somiglianze e differenze con la speranza di trovare quella differenza risolutiva che potesse portare alla conclusione assurda.

Il mio centesimo l'ho messo, ora sta a voi continuare!

Contents

1	Introduzione	1
2	Considerazioni preliminari	2
3	Teoremi di Fermat ed Eulero	4
4	Coprimalità e sue proprietà	4
5	Questioni di divisibilità	7
6	Lemmi notevoli	11
7	Fattorizzazione del parametro α	18
8	Espressione analitica del parametro α	19
9	Riscoperta delle formule di Barlow	21
10	Conclusioni	24

List of Tables

References

- [1] Claudio Beccari, *LaTeX, Guida ad un sistema di editoria elettronica*, Editore Ulrico Hoepli, Milano, 1991
- [2] Paulo Ribenboim, *Fermat's Last Theorem For Amateurs*, Springer-Verlag New York, Inc., 1999